普通高等学校本科专业设置申请表



校长签字：

学校名称（盖章）：山西大学

学校主管部门：山西省

专业名称：网络空间安全

专业代码：080911TK

所属学科门类及专业类：工学 计算机类

学位授予门类：工学

修业年限：四年

申请时间：2025-07-04

专业负责人：耿海军

联系电话：13934658692

教育部制

1. 学校基本情况

学校名称	山西大学	学校代码	10108
主管部门	山西省	学校网址	www.sxu.edu.cn
学校所在省市区	山西太原小店区坞城路92号	邮政编码	030006
学校办学基本类型	□教育部直属院校 □其他部委所属院校 ☑地方院校 ☑公办 □民办 □中外合作办学机构		
已有专业学科门类	☑哲学 ☑经济学 ☑法学 ☑教育学 ☑文学 ☑历史学 ☑理学 ☑工学 □农学 □医学 ☑管理学 ☑艺术学		
学校性质	☑综合 □理工 □农业 □林业 □医药 □师范 □语言 □财经 □政法 □体育 □艺术 □民族		
曾用名	无		
建校时间	1902	首次举办本科教育年份	1902年
通过教育部本科教学评估类型	审核评估	通过时间	2024年11月
专任教师总数	2285	专任教师中副教授及以上职称教师数	1421
现有本科专业数	87	上一年度全校本科招生人数	6570
上一年度全校本科毕业人数	5799		
学校简要历史沿革	山西大学前身为创建于1902年的山西大学堂。1998年成为山西省重点建设大学；2005年成为最早的一批省部共建大学；2012年成为“中西部高校综合实力提升工程”入选高校；2018年成为教育部和山西省人民政府共同建设的部省合建高校；2022年进入国家“双一流”建设高校行列。		
学校近五年专业增设、停招、撤并情况	学校按照“控量提质增效，扶优扶强扶特”的总体思路，优化本科专业结构布局，进一步提升专业核心竞争力。2020年停招汉语国际教育、学前教育、工程管理3个专业，增设智慧建筑与建造1个专业；2021年停招社会工作、建筑学、建筑电气与智能化、电子商务、经济统计学5个专业，增设合成生物学、人工智能2个专业；2022年停招工程造价1个专业，增设生态学1个专业；2023年撤销酒店管理、社会学2个专业；2024年撤销劳动与社会保障、环境生态工程、社会体育指导与管理、公共艺术、物业管理等5个专业，申请增设纪检监察、“政治学、经济学与哲学（PPE）”“马克思主义理论		

	”“数据科学”等4个专业。

2.申报专业基本情况

申报类型	新增国控专业		
专业代码	080911TK	专业名称	网络空间安全
学位授予门类	工学	修业年限	四年
专业类	计算机类	专业类代码	0809
门类	工学	门类代码	08
申报专业类型	新建专业	原始专业名称	-
所在院系名称	自动化与软件学院		
学校现有相近专业情况			
相近专业1专业名称	软件工程	开设年份	2005年
相近专业2专业名称	计算机科学与技术（注：可授理学或工学学士学位）	开设年份	1980年
相近专业3专业名称	-	开设年份	-

3.申报专业人才需求情况

申报专业主要就业领域	网络空间安全专业毕业生就业领域广阔。在政府机构，参与网络安全管理与网络犯罪侦查，维护国家网络安全。在金融机构，负责金融数据安全，保障交易安全。在互联网和通信企业，从事技术研发、运维和安全评估，确保网络服务稳定。在安全企业，担任网络安全工程师、渗透测试工程师等，为企业提供专业服务。科研与教育领域也欢迎该专业毕业生，学生可以攻读更高学位，进行前沿技术研究，培养专业人才。随着新兴技术如物联网和人工智能的崛起，也为该专业毕业生提供了更多机会，学生可专注于该领域的安全设计、评估和防御。未来3-5年，具备实战技能的安全运维人员与高水平专家将成为稀缺资源。综上所述，网络空间安全专业毕业生凭借扎实的专业知识和实践能力，能在就业市场中发挥关键作用，为国家网络安全贡献力量，同时实现个人职业发展。
人才需求情况	随着网络空间安全在各行业的广泛应用，政府单位、社会公共服务机构及企业对网络安全的重视程度日益提高，纷纷建立网络安全技术团队或委托专业服务团队来保障网络安全。据《2024 网络安全产业人才发展报告》及《网

	络安全人才实战能力白皮书》显示，我国网络安全人才缺口巨大，预计到2027年缺口将达327万，而高校人才培养规模仅为3万/年，且92% 的企业表示缺乏实战型人才。在山西，数字化转型的推进也使得对网络安全人才的需求日益迫切，众多用人单位加大了对网络安全专业人才的引进力度。新兴领域的发展也为网络安全人才带来了新的机遇，如人工智能领域，随着人工智能技术在网络安全中的广泛应用，对相关人才的需求日益增长，用人单位需要具备机器学习、深度学习等算法安全性分析与攻击防御能力的人才，同时要能设计并实现高效安全防护策略，防止数据泄露等问题。 为深入了解用人单位对网络空间安全专业人才的需求情况，山西大学进行了广泛调研。以下是一些用人单位的网络安全人才需求预测情况： 北京天融信教育科技有限公司的需求量为15人，国信蓝桥教育科技股份有限公司的需求量为15人，昆山杰普软件科技有限公司的需求量为10人，山西信思智学教育科技有限公司的需求量为10人，山西软赢科技有限公司的需求量为5人。这些岗位主要涉及安全工程师、安全研究员、安全咨询师、网络安全运维、安全监测与应急响应、软件安全开发、安全测试、安全评估、网络安全培训教学、课程研发、培训项目交付等多个方向，要求毕业生具备扎实的网络安全基础知识和实践经验，能够熟练运用各类网络安全技术和工具，为企业提供网络安全解决方案和安全保障服务，或者具备网络攻防实战能力、代码审计、漏洞挖掘与修复等能力，以满足不同用人单位的实际业务需求。 该专业在山西大学的设立，将立足山西，面向全国，为山西地区乃至全国培养出一批具有扎实专业知识和实践能力的网络安全人才，有效缓解人才短缺的问题。通过系统的课程设置和实践教学，学生可以掌握网络安全的核心技术和实战技能，毕业后能够迅速适应工作岗位的需求。山西大学将加强与用人单位的紧密合作，深入了解行业需求，为学生提供丰富的实习和就业机会，拓宽学生的就业渠道，同时也为山西省的网络安全产业和数字经济发展提供有力的人才支撑，促进山西地区网络安全产业的繁荣发展，提升山西省在网络安全领域的整体竞争力。	
申报专业人才需求调研情况	年度招生人数	70
	预计升学人数	15
	预计就业人数	55
	北京天融信教育科技有限公司	15
	国信蓝桥教育科技股份有限公司	15

	昆山杰普软件科技有限公司	10
	山西信思智学教育科技有限公司	10
	山西软赢科技有限公司	5

4. 产业调研报告

关于申报网络空间安全专业的行业产业调研报告

一、调研背景与目的

1、背景

随着全球数字化进程加速，云计算、物联网、人工智能等新兴技术深度融入经济社会各领域，网络空间已成为继陆、海、空、天之后的“第五大战略空间”。与此同时，网络攻击手段持续升级，数据泄露、勒索软件、供应链攻击等安全事件频发，对国家安全、社会稳定、经济发展构成严峻挑战。

（1）国家战略升级，网络安全成为发展基石

当前，我国将网络安全定位为国家安全的核心组成，“没有网络安全就没有国家安全”已成为国家数字化发展的根本原则。党的二十大明确提出“构建全域联动、立体高效的国家安全防护体系”，网络安全产业被纳入国家战略性新兴产业体系。随着《网络安全法》、《数据安全法》、《个人信息保护法》等法规密集落地，行业进入强合规驱动时代，政企机构对安全能力建设需求激增。

（2）产业规模爆发式增长，人才缺口持续扩大

2023 年我国网络安全产业规模达 992 亿元，同比增长 7%，2024 年突破千亿规模，2025 年预计达到 1244 亿元。与此同时，人才供需矛盾尖锐：据工信部预测，2025 年网络安全人才缺口将突破 200 万，其中应用型、复合型人才占比超 70%。尤其在人工智能安全、数据隐私保护、工业互联网安全等新兴领域，具备实战能力的专业人才极度稀缺。

（3）技术迭代加速，倒逼人才培养体系改革

攻击形态向 APT、勒索软件、AI 生成攻击演进，防御技术向主动化、智能化升级（如蜜网体系、零信任架构、抗量子密码）。然而当前高校培养存在课程滞后于技术、实践脱离场景、能力匹配不足三大痛点。企业反馈显示，应届毕业生需平均 6 个月重新培训方能胜任基础安全运维，反映出教育供给侧与产业需求侧的错位。

2、目的

本报告旨在剖析网络空间安全行业的产业规模、技术热点、人才供需、政策环境及竞争格局，明确行业发展瓶颈与机遇。通过聚焦核心产业链环节（如安全

硬件、软件、服务）和新兴领域（如云安全、工控安全、AI 安全），提出针对性发展策略，为我校优化人才培养体系提供决策参考，助力构建自主可控的网络空间安全防护体系。

二、调研对象与方法

1.调研对象

本次调研的对象主要包括以下几类实体：

（1）调研了国家网络安全主管部门、行业监管机构以及执法部门，这些部门在政策制定与合规要求方面发挥着关键作用。通过与这些机构的沟通，我们了解到国家对网络空间安全的重视程度不断提升，相关法规如《网络安全法》《数据安全法》《个人信息保护法》等的密集落地，促使政企机构对安全能力建设的需求激增，这也为网络空间安全专业人才提供了广阔的就业空间。

（2）调研了高校网络安全专业院系及科研院所，这些机构在人才培养与技术研发方面具有丰富的经验和资源。例如，太原理工大学、江苏大学、郑州大学等高校的网络空间安全专业建设情况，为山西大学的专业设置提供了宝贵的参考。这些高校在课程设置、实践教学、师资队伍建设等方面的经验，有助于山西大学优化自身的专业培养体系。

（3）调研了北京天融信教育科技有限公司、国信蓝桥教育科技股份有限公司、昆山杰普软件科技有限公司、山西信思智学教育科技有限公司和山西软赢科技有限公司等，这些企业不仅提供了行业前沿的技术动态和市场需求信息，还明确表示了对网络空间安全专业人才的需求。其中，北京天融信教育科技有限公司的需求量为 15 人，国信蓝桥教育科技股份有限公司的需求量为 15 人，昆山杰普软件科技有限公司的需求量为 10 人，山西信思智学教育科技有限公司的需求量为 10 人，山西软赢科技有限公司的需求量为 5 人。这些企业对具备实战技能和扎实专业知识的人才需求迫切，尤其在安全工程师、安全研究员、安全咨询师、网络安全运维、安全监测与应急响应等岗位上。

（4）调研了金融、电信、能源等关键信息基础设施行业用户，以及中小企业代表，分析其安全需求与实践。这些行业用户对网络空间安全的需求日益增长，尤其是在数据保护、系统安全、网络安全等方面。例如，金融机构需要专业的网络安全人才来保障金融交易的安全，能源企业需要应对日益复杂的工业控制系统

安全威胁。通过与这些行业用户的交流，我们了解到他们对网络空间安全专业人才的技能要求和岗位需求，为专业设置提供了实际依据。

2.调研方法

本次调研采用多维度方法，确保数据全面性与可靠性：

（1）系统查阅了国内外权威行业报告、政策文件、学术期刊及企业年报，分析了市场规模、技术趋势与政策环境。通过文献调研，我们了解到网络空间安全产业的快速发展态势，以及我国在网络安全人才方面的巨大缺口。例如，据《2024网络安全产业人才发展报告》及《网络安全人才实战能力白皮书》显示，我国网络安全人才缺口巨大，预计到2027年缺口将达327万，而高校人才培养规模仅为3万/年。

（2）设计了结构化问卷，通过线上平台分发至目标企业、用户及机构，收集了定量数据。问卷内容涵盖了企业对网络空间安全专业人才的需求量、岗位要求、技能需求等方面。通过问卷调查，我们收集到了大量企业的真实需求数据，为专业设置提供了有力支持。

（3）对网络安全企业高管及专家学者进行了半结构化访谈。访谈内容包括企业对网络空间安全专业人才的实际需求、行业面临的挑战与机遇等。例如，与北京天融信教育科技有限公司的高管访谈中，我们了解到该公司对具备实战能力的网络安全人才的迫切需求，以及他们在人才培养和使用方面的经验。

（4）选取了代表性企业或项目进行实地考察与案例研究，验证了行业实践。通过对这些企业或项目的实地考察，我们深入了解了网络空间安全技术在实际中的应用情况，以及企业在人才培养和使用方面的成功经验。

（5）整合了公开数据源进行定量分析，结合SWOT模型评估了产业现状与发展潜力。通过对数据的分析，我们明确了网络空间安全行业的优势、劣势、机会和威胁，为专业设置和发展提供了科学依据。

三、行业产业发展现状与趋势

随着数字化进程的加速推进和新兴技术的迅猛发展，网络空间安全已成为国家安全体系的重要组成部分。

在数字经济成为全球经济增长新引擎的背景下，网络空间安全已从单纯的技术问题上升为关乎国家,安全、经济发展和社会稳定的核心议题。2025年作为”

十四五"规划的收官之年和"十五五"规划的谋划之年，我国网络空间安全领域正站在前所未有的历史交汇点上。随着《国家数据基础设施建设指引》《网络数据安全管理条例》等政策法规的密集落地，"数字中国"战略深入推进，网络空间安全专业的发展迎来了重大机遇与挑战。

当前，全球网络安全形势日趋复杂，网络安全事件频发，网络攻防不平衡加剧，同时，我国网络安全市场，规模持续扩大，预计 2025 年全球规模将突破 3000 亿美元，同比增长 12%。在此背景下，网络空间安全专业肩负着培养高素质人才、突破核心技术、构建安全屏障的重要使命。

1、网络空间安全专业人才培养现状

我国网络空间安全人才培养体系经过多年建设已初具规模，形成了多层次、多类型的教育培训格局。从总体上看，人才培养工作取得了显著成效，但在供需对接、质量提升等方面仍有优化空间。

（1）政策标准体系日趋完善

近年来，我国高度重视网络安全人才培育工作，通过一系列政策规划和产业协同举措，持续提升网络安全人才供给能力。2016 年，中央网信办等六部门发布《关于加强网络安全学科建设和人才培养的意见》，为网络安全学科建设和系统性人才培养明确了方向指引。此后，《网络安全法》《数据安全法》对网络安全相关教育与培训工作提出了更为精细、明确的要求。2024 年，人力资源社会保障部等九部门发布《加快数字人才培育支撑数字经济发展行动方案(2024-2026年)》，提出构建覆盖安全领域的"职业标准制定-能力培训评价-职称体系衔接"三位一体职业发展体系。

在标准体系方面，《中华人民共和国职业分类大典(2022 年版)》新增了数据安全工程技术人员、密码工程技术人员、网络与信息安全管理员等网络安全相关职位。国家市场监督管理总局、国家标准化管理委员会联合发布的《信息安全技术网络安全从业人员能力基本要求》则明确了网络安全岗位的分级与能力要素。这些政策标准为网络安全人才培养提供了制度保障和发展框架。

（2）市场需求呈现多元化特征

伴随网络技术向各行业纵深渗透，网络安全领域范畴持续延展，岗位需求呈现多元化、专业化发展趋势和特点。技术类人才需求尤为强烈，安全运维工程师、

安全开发工程师、渗透测试工程师成为招聘需求第一梯队。这些岗位要求工程师具备主动防御以及应对动态安全威胁的能力，其专业实操技能水平直接关系到企业能否有效抵御外部风险。从地域分布看，网络安全岗位需求主要集中在北京、上海、深圳等一线城市。这些城市凭借经济发展水平、科技产业基础和创新创业氛围，成为网络安全从业者的首选就业地，形成了显著的人才集聚效应。企业用人标准也日趋综合化，近四成网络安全岗位将1-2年工作经验列为招聘必备条件。除专业技能外，沟通能力、团队协作及学习能力等非学历特质也被纳入考量范畴。这表明企业对网络安全人才的要求已从单一技术能力向综合素质拓展。

（3）教育供给体系逐步健全

我国网络安全教育体系逐渐完善，学科专业与课程建设力度持续加大。据统计数据，截至2024年，全国共有626所高校开设网络安全相关专业，覆盖全国普通高校总数的21.8%，其中本科院校283所、高职院校343所。行业在岗培养机制也在不断完善。超过六成网络安全从业者所在企业已构建任职标准体系。

总体而言，我国网络空间安全人才培养已建立起较为完整的体系框架，政策支持力度不断加大，教育供给规模持续扩展，行业需求导向日益明确。然而，人才培养质量与产业实际需求间仍存在一定差距，特别是在高端领军人才储备、实战能力培养、评价认证体系等方面还有较大提升空间。

2、网络空间安全技术发展现状与产业应用

网络空间安全技术作为保障数字经济发展的核心支撑，正处于快速演进阶段。当前，以人工智能、云计算为代表的新兴技术正在深刻重塑网络安全防护模式，推动产业从被动防御向智能主动防御转变。

（1）人工智能深度赋能网络安全

2025年，AI技术发展进一步加剧了网络攻防不平衡的状况，以AI对抗AI已成为企业的必选项。AI不仅在安全运营领域逐步普及，还在攻防安全渗透测试、漏洞分析与挖掘、数据安全、代码安全等领域得到深化应用，使得网络攻防对抗更加复杂多变。

（2）数据安全与隐私保护技术进展

随着《国家数据基础设施建设指引》等政策出台，构建从基础设施、算力网底座到数据应用的全流程保护体系成为数据安全建设重点。数据安全技术正从静

态保护向动态保护、从边界安全向内生安全、从封闭环境保护向开放环境保护转变，形成贯穿数据全生命周期的动态安全防护能力。

在数据基础设施安全方面，加强可信接入、安全互联、跨域管控和全栈防护等安全管理至关重要。需要建立网络安全风险和威胁的动态发现、实时告警、全面分析、协同处置、跨域追溯和态势掌控能力，并提供应对芯片、软件、硬件、协议等内置后门、漏洞安全威胁的内生防护能力。

（3）云安全与物联网安全技术演进

云安全架构正在经历重大变革，国内云计算市场已进入新阶段，企业对云服务的需求从简单资源获取转向深度应用和创新。云安全领域也从单纯满足合规要求向具备实战能力的方向发展，实战化的云安全防护能力成为企业选择云服务提供商的重要考量因素。

物联网安全面临新的挑战。到2025年，全球物联网设备连接数量预计将超过250亿个。智能门锁被黑客破解、智能摄像头被用于窃取隐私等事件频发，揭示了物联网安全问题的严峻性。企业需要加强物联网设备的加密通信、访问控制、定期更新固件等安全管理措施。

（4）工业控制系统与供应链安全技术

工业控制系统作为国家关键基础设施的"大脑"，其安全性直接关系到国家的经济安全和社会稳定。利用安全软件供应链开展的攻击存在造成大范围系统崩溃瘫痪的风险.

总体而言，当前网络空间安全技术呈现智能化、集成化、实战化等特征。人工智能深度赋能各安全场景，云安全、数据安全等技术趋向平台化整合，而日益严峻的威胁形势则推动技术发展更加注重实战效果。未来，随着量子计算、6G通信等新兴技术的成熟，网络安全技术体系还将面临新一轮的革新与挑战。

3、网络空间安全专业发展趋势分析

随着数字化转型的持续深入和新兴技术的快速演进，网络空间安全领域正在经历深刻变革。准确把握未来发展趋势，对于优化人才培养方向、调整科研重点、布局产业战略具有重要意义。

（1）AI重塑网络攻防格局

人工智能将继续深度赋能网络安全各领域，推动防护模式从规则驱动向智能

自主演进。AI 的持续学习能力使其能够不断适应新的威胁模式，为网络安全提供动态、智能的防护屏障。AI 将全面融入安全运营流程，解放安全团队生产力。面对 AI 时代外部威胁加剧、安全运营效率低下和安全人员短缺的问题，数智化程度较高、业务高度依赖 IT 系统的政企客户会加快将 AI 能力应用到安全运营工作流程中，自动化繁琐的初级任务。同时，业内将推动构建基于 AI 的统一数据访问标准，使 AI 能访问从网络、端点、云和应用中收集的全方位信息和数据，提高准确决策及执行任务的能力。

（2）数据基础设施全流程保护

随着《国家数据基础设施建设指引》等政策出台，构建从基础设施、算力网底座、数据应用，以及数据流通利用等贯穿从底层到应用层的全流程保护体系，成为数据安全建设重点。党的二十届三中全会明确指出要"建设和运营国家数据基础设施，促进数据共享"。展望 2025 年，围绕数据基础设施的安全建设将聚焦四大方向：为国家数据基础设施打造内生防护能力，筑牢安全底座；为国家算力网基础平台提供一体化的安全保障服务能力；构建全链条的数据安全动态防护体系；为数据流通利用构筑安全可信的环境。

（3）网络安全技术自主可控

在全球化背景下，网络安全技术自主可控对于维护国家网络安全具有重要意义。近年来，一些国家在网络安全技术上过度依赖他国，导致在关键时刻遭受网络攻击时难以有效应对。国家将加大自主研发力度，推动网络安全技术的自主可控发展。加大对网络安全技术研发的投入和支持力度；企业将积极参与网络安全技术研发和创新活动；同时加强产学研合作，推动网络安全技术的成果转化和应用。

（4）实战型人才培养成为核心

未来网络安全人才培养将更加注重实战能力和创新思维。培养网络安全领军人才。

综合来看，网络空间安全专业未来发展将呈现技术智能化、防护体系化、人才实战化的总体特征。AI 技术将深度重构安全防护模式，数据基础设施的全流程保护日益重要，而自主可控技术和实战型人才培养则是应对复杂安全形势的关键保障。准确把握这些趋势，对于规划网络空间安全专业发展路径、优化资源配

置具有重要指导意义。

四、行业产业人才需求分析

网络空间行业作为数字经济时代的核心支柱之一，涵盖网络安全、云计算、大数据、人工智能、物联网等多个领域，其人才需求呈现快速扩张和持续迭代的特点。

（1）行业发展情况

各国将网络空间安全上升为国家战略，催生合规性人才需求，新基建、东数西算等工程拉动云计算、数据中心领域、5G、AI 等新技术带来新型安全威胁，数字化转型推动企业上云，云计算和混合架构人才需求等信息技术行业继续发展，加大高质量行业人才需求。同时，全球网络攻击频发，加大网络安全人才需求缺口。据国际信息系统安全认证联盟发布的《2023 年全球网络安全人才发展报告》显示，全球网络安全人才规模达到 550 万人，同比增长 8.7%，然而人才缺口却进一步扩大到 400 万人，平均增长 12.6%，特别是在亚太地区，网络安全人才短缺人数同比增长 23.4%。而我国网络安全人才供需失衡问题更为严峻，据教育部发布的《网络安全人才实战能力白皮书》指出，预计到 2027 年，我国网络安全人员缺口将达到 327 万，而高校每年的人才培养规模仅为 3 万。

（2）人才需求特征

技术复合型及跨领域人才需求增长，如面向“安全+AI”的网络安全威胁的智能分析、“云+安全”的云原生安全架构师等。

实战能力要求提高，相关人才需具备攻防演练、漏洞挖掘等实践经验，具有相关资质或经历的求职者更受企业青睐。

岗位细分深化，传统岗位（如渗透测试、SOC 分析）之外，新兴岗位如数据安全工程师、隐私保护专家、车联网安全研究员人才需求增长。

地域分布不均，一线城市（北深杭沪）聚集 70%以上岗位，中西部面临人才流失。

综合技能要求提升，从业人员需具备风险沟通能力（向非技术管理者解释威胁）、项目管理（如安全体系建设）、法律意识（合规性设计）等综合素质。

（3）核心岗位方向

安全体系架构师，设计企业级安全架构，制定安全技术路线，精通零信任架

构、云原生安全框架。

业务安全分析师，识别业务系统脆弱性，设计风控策略，熟悉金融/电商等垂直领域业务流程。

安全开发工程师，开发安全产品组件，实现安全功能模块。

代码审计工程师，检测代码漏洞，制定安全编码规范。

安全运维工程师，日常系统加固、漏洞扫描与策略维护，熟练配置防火墙/WAF/IDS，Linux 系统管理。

数据安全管理工程师，实施数据分级保护，保障数据全生命周期安全，熟悉 GDPR/CCPA 及《数据安全法》合规要求。

渗透测试工程师，模拟攻击挖掘漏洞，提供修复方案。

应急响应工程师，处置安全事件，溯源攻击链，精通日志分析（ELK）、内存取证技术。

威胁情报分析工程师，追踪 APT 组织，输出预警报告，熟悉 MISP 平台，掌握溯源反制技术。

安全合规评估工程师，执行等保测评，推动合规整改，熟悉 ISO 27001/等保 2.0 标准。

安全风险管理工程师，评估企业安全风险，制定防控策略，掌握风险管理框架。

（4）发展趋势

技能动态化，随着 AI 自动化工具（如 SOAR、低代码安全）普及，基础运维岗位需求下降，高阶分析/设计岗需求上升。

全球化高端人才竞争，跨国企业争夺顶尖人才。

产教融合加速，政企校合作模式（如“网络安全学院+创新产业园”）将成为人才供给主渠道，提高人才培养质量。

网络空间行业的人才需求将持续向技术深度与行业广度双向扩展，未来仍将处于供需失衡状态。网络空间作为第五大主权空间，其安全直接关乎国家核心利益，提升网络空间安全专业人才培养具有重要的战略意义。

五、同类高校专业建设情况调研

与山西大学同类的高校通常是指在综合实力、学科水平等方面相近的地方高校，如太原理工大学、南昌大学，河南大学等。以下是这些高校网络空间安全专业的建设情况：

（1）太原理工大学：太原理工大学计算机科学与技术学院（大数据学院）设有网络空间安全本科专业，拥有计算机科学与技术博士后流动站，计算机科学与技术一级学科博士和硕士授权点，以及网络与信息安全二级学科专业硕士授权点。学校还建有工业互联网安全山西省工程研究中心和工业互联网安全山西省重点实验室，为专业建设提供了有力的科研平台支持。

（2）江苏大学：江苏大学计算机科学与通信工程学院设有网络空间安全专业。学院拥有计算机科学与技术一级学科硕士学位授权点、软件工程一级学科硕士学位授权点等。网络空间安全专业依托学院的学科平台，注重培养学生掌握网络空间安全相关的基础理论和专业知识，具备网络安全防护、数据安全保障等能力，为网络空间安全领域输送专业人才。

（3）郑州大学：网络空间安全学院构建了 “选拔 — 培养 — 评价” 全过程创新拔尖人才培养体系，设立网络主动防御、网络与系统安全等六个培养方向。2025 年获批国家级人才培养基地，开设嵩山实验班，创新 “4+2” 本硕联培培养机制。学院与网安头部企业奇安信筹建奇安信学院，学生在全国大学生信息安全竞赛等赛事中屡获佳绩。

（4）安徽大学：网络空间安全专业开设在互联网学院，致力于培养能够支撑和引领国家网络空间安全领域的拔尖创新人才和行业高级工程人才，注重学生工程实践能力培养，使其能从事网络空间相关软硬件开发、系统设计等工作。

（5）河北大学：河北大学是河北省重点综合性大学，其网络空间安全专业依托计算机科学与技术学院建设。学院拥有较为完善的教学设施和科研平台，专业注重培养学生的网络安全基础理论和实践能力，课程设置涵盖密码学、网络安全技术等方面，致力于为京津冀地区培养网络空间安全专业人才。

（6）河南大学：计算机与信息工程学院设有网络空间安全相关专业或方向，借助学校的学科综合优势，强调学科交叉融合，培养学生掌握网络空间安全核心技术，具备网络安全管理、安全攻防等能力，为地方和国家网络安全事业输送人才。

（7）南昌大学：南昌大学作为江西省的重点高校，信息工程学院设有网络空间安全专业。学院拥有多个省级科研平台，为专业建设提供了支撑。专业致力于培养具有扎实网络空间安全理论基础和实践能力的人才，注重与企业合作，开展产学研协同育人，提高学生的工程实践能力和就业竞争力。

（8）福州大学：是国家 “双一流” 建设高校，其网络空间安全专业建设依托计算机科学与技术学科。学校设有相关科研机构，在网络安全攻防、密码技术等领域开展研究，专业课程体系完善，注重培养学生的创新能力和实践技能，为福建省及全国培养网络空间安全专业人才。

（9）云南师范大学：于 2024 年开设网络空间安全专业，隶属于信息学院。该专业旨在培育德才兼备的专业人才，要求学生掌握人文社科、自然科学及信息科学基础知识，扎实掌握网络空间安全理论，具备网络与信息安全系统设计、开发与应用能力，熟悉工程项目流程，未来可在政产学研用等多领域，从事科研、开发、管理等工作。

六、我校申报网络空空间安全新专业的必要性与可行性分析

1、必要性

网络空间已成为继陆、海、空、天之后的第五大主权领域空间，其安全问题直接关系到国家安全、社会稳定以及个人隐私保护等诸多重要方面。在当今数字化时代，网络攻击、数据泄露等安全事件频发且愈发严重，给国家、企业和个人带来了不可估量的损失。据国际信息系统安全认证联盟发布的《2023 年全球网络安全人才发展报告》显示，全球网络安全人才规模达到 550 万人，同比增长 8.7%，然而人才缺口却进一步扩大到 400 万人，平均增长 12.6%，特别是在亚太地区，网络安全人才短缺人数同比增长 23.4%。而我国网络安全人才供需失衡问题更为严峻，据教育部发布的《网络安全人才实战能力白皮书》指出，预计到 2027 年，我国网络安全人员缺口将达到 327 万，而高校每年的人才培养规模仅为 3 万。面对如此庞大的人才需求缺口，山西大学增设网络空间安全专业显得尤为必要。这不仅是对国家战略需求的积极响应，能够为国家培养出一批具备扎实理论基础、较强实践能力和创新精神的专业人才，服务于网络强国建设，保障国家网络安全和信息安全，同时也契合了行业发展趋势，为地方经济建设和行业发展输送急需的专业人才，推动区域经济的数字化转型和高质量发展。

增设网络空间安全专业将为学生提供一个系统学习网络空间安全知识和技能的平台，使学生能够深入掌握网络空间安全领域的基本理论和方法，具备扎实的专业知识和技能。通过专业学习，学生将具备较强的网络攻防实战能力、安全系统设计与开发能力以及安全策略制定与实施能力，能够适应网络空间安全领域的科研机构、高校、企业、政府机关等单位的工作需求。同时，学校注重培养学生的科学素养和创新意识，使学生能够跟踪网络空间安全领域的前沿技术和发展动态，开展前沿性的科研工作。此外，学校还注重培养学生的团队协作精神和沟通能力，使学生能够在跨学科、跨领域的团队中发挥作用，共同解决复杂的网络空间安全问题。

随着网络空间安全行业的发展，对专业人才的需求不断增长，为学生提供了广阔的就业空间和发展机会。山西大学网络空间安全专业的学生在毕业后，凭借在学校所学的专业知识和技能，将能够在各大企事业单位、政府部门从事网络安全相关工作，如网络安全工程师、渗透测试工程师、安全咨询顾问等职位。学校与多家知名企业的合作关系也将为学生提供更多的就业机会和职业发展空间，提高学生的就业竞争力。

增设网络空间安全专业将进一步提升山西大学在网络空间安全领域的学科影响力和综合实力，为学校的发展注入新的活力。同时，该专业的建设也将为社会培养出更多优秀的网络空间安全专业人才，满足国家对网络安全人才的迫切需求，为维护国家网络安全和社会稳定做出积极贡献。此外，学校通过开展网络空间安全教育和科研，将推动网络空间安全技术的发展和创新，为网络空间安全产业的发展提供技术支持和智力保障。

2、可行性

山西大学增设网络空间安全专业的计划紧密契合国家战略需求、行业发展趋势以及学校自身的学科布局规划。从宏观层面来看，随着信息技术的飞速发展，网络空间安全已成为国家安全战略中的关键一环，国家对网络安全专业人才的需求迫在眉睫，山西大学增设该专业能够为国家培养出一批具备扎实理论基础、较强实践能力和创新精神的专业人才，为网络强国建设提供有力的人才支撑。从行业需求角度分析，当前全球数字经济蓬勃发展，各关键行业对网络空间安全的重视程度不断提高，对网络安全专业人才的需求呈现出爆发式增长，而高校现有的

人才培养规模远远不能满足市场需求。山西大学增设网络空间安全专业，能够为地方经济建设和行业发展培养急需的专业人才，促进区域经济的数字化转型和高质量发展。从学校自身发展来看，山西大学作为一所学科门类齐全的综合性大学，在多个学科领域都具有较高的教学和科研水平。增设网络空间安全专业将进一步完善学校的信息学科布局，促进学科间的交叉融合与协同发展。网络空间安全专业与学校的计算机科学与技术和软件工程等相关学科紧密相连，相互支撑。通过整合优势资源，学校可以在网络空间安全领域形成从本科到硕士、博士的完整人才培养体系，提升学校在网络空间安全领域的学科影响力和综合实力。

（1） 学科平台优势

山西大学于 2019 年获批网络空间安全一级学科硕士学位授权点，成为山西省首批拥有该授权点的高校之一。学校在网络空间安全领域已构建起较为完善的学科平台体系，包括 2 个省级工程技术研究中心、2 个省级研究生教育创新中心、1 个省级创新团队以及 2 个山西省国际合作基地与平台项目。这些优质平台为师生提供了广阔的科研空间和丰富的实践机会，极大地推动了网络空间安全学科的建设和发展。山西大学的计算智能与中文信息处理教育部重点实验室、复杂系统与数据科学教育部重点实验室等，为开展前沿性的网络空间安全研究提供了坚实的基础和良好的科研条件。

（2）师资队伍实力

学校在网络空间安全学位点领域汇聚了一支高水平师资队伍，现有专任教师 21 名，其中教授 5 名，博导 3 名，硕导 18 名，具有博士学位的教师 18 名，获外单位硕士及以上学位的比例为 85.71%，35 岁及以下有 6 人，比例为 28.57%。教师们在网络安全领域具有深厚的学术造诣，已在国内外学术期刊和会议上发表了多篇高质量的学术论文，并主持了多项国家级和省级科研项目，为网络空间安全专业的教学和科研提供了有力保障。

（3）教学资源与实践条件

学校高度重视网络空间安全专业的教学资源建设，配备了先进的实验教学设备和专业软件，建设了包括集群 NAS 存储系统、数据中心平台、高性能计算平台、网络攻防演练平台、软件定义网络平台等在内的多个高水平实验室。这些实验室为学生提供了理论与实践相结合的学习环境，使学生能够在实际操作中掌握网络

空间安全的核心技术和技能。此外，学校与北京天融信教育科技有限公司等一流网络安全企业建立了长期稳定的合作关系，为学生提供了丰富的实践教学基地和就业机会。学校与企业共建的校外实践基地，为学生提供了参与实际网络安全项目的实践机会，有效提升了学生的实践能力和解决实际问题的能力。

（4）人才培养成果

网络空间安全学位点致力于培养“高层次应用型创新人才”，重视学生创新意识与实践能力培养。首届硕士研究生学位论文盲审合格率 100%，顺利毕业且 100%就业，就业领域广泛，体现学科培养的普适性与实用性，且学科积极支持研究生到国外高水平大学联合培养，2024 年 10 月已经选派 3 名研究生前往奥克兰大学进行联合培养。为激发研究生学术兴趣等，学位点在多层面建立规定要求及激励机制，提供良好条件，如组织参加学科竞赛、选拔参加联合培养、鼓励参与科研项目等。近三年，研究生发表 SCI/EI、中文核心等学术论文 30 余篇，申请专利 20 余项，获各类学科竞赛奖 10 余项，综合素质显著提升，学位点的持续创新力和竞争力也得到增强。

（5）学科方向与发展

山西大学网络空间安全学科已形成网络与系统安全、应用与数据安全及新型信息技术安全两大研究方向。在网络与系统安全方面，主要研究工业控制系统的网络安全态势感知与防御、工业控制系统软件安全等，针对工业控制系统网络安全系统存在的漏洞难发现、攻击难溯源、防护易突破等挑战，研发工业控制系统网络攻击的防护技术，搭建相应的网络安全态势感知与防护平台。在应用与数据安全及新型信息技术安全方面，主要研究物联网和智能设备在信息物理系统中的安全与隐私保护，针对山西省智能制造、智慧城市、智能家居和无人系统等技术领域，解决复杂系统中的设备交互逻辑复杂性、安全脆弱性累积风险和设备管理策略的冲突问题，研发集成监控和干预的综合平台，提升数据安全性。学科还保持与国内外顶尖学者在新型电力系统、物联网和智能设备等关键领域的合作与交流，确保在网络空间安全研究领域的前瞻性和技术开发的实力性，培养的人才能够满足市场需求。

七、结论与建议

1、结论

山西大学增设网络空间安全专业具有充分的理由和扎实的基础。学校在网络空间安全领域已具备完善的学科平台、高水平的师资队伍、丰富的教学资源与实践条件，以及显著的人才培养成果。增设该专业将进一步完善学校的信息学科布局，促进学科间的交叉融合与协同发展，提升学校在网络空间安全领域的学科影响力和综合实力。同时，该专业的建设将为国家和社会培养更多优秀的网络空间安全专业人才，满足国家对网络安全人才的迫切需求，为维护国家网络安全和社会稳定做出积极贡献。

2、建议

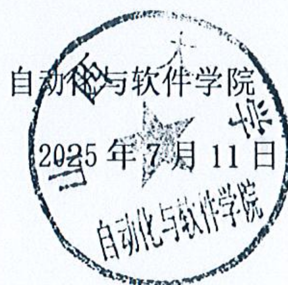
（1）加强师资队伍建设：进一步引进和培养高水平的师资队伍，特别是具有实战经验和行业背景的教师，提升教师的教学水平和科研能力。

（2）优化课程体系：根据行业需求和技术发展动态，及时调整和优化课程设置，增加实践教学比重，注重培养学生的实战能力和创新思维。

（3）深化产教融合：加强与网络安全企业的合作，建立更多的校外实践基地，为学生提供丰富的实践机会和就业渠道。同时，积极开展产学研协同创新，推动网络空间安全技术的成果转化和应用。

（4）加强国际合作与交流：积极参与国际学术交流与合作，与国外高水平大学和科研机构建立合作关系，选派优秀学生和教师到国外交流学习，提升学校的国际化水平。

（5）加大政策支持与投入：学校应加大对网络空间安全专业的政策支持和经费投入，完善教学设施和科研平台，为专业的建设和发展提供有力保障。



自动化与软件学院

2025 年 7 月 11 日


扫描全能王 创建

5. 申请增设专业人才培养方案

网络空间安全专业培养方案

（专业代码：080911TK）

一、专业简介（Major Overview）

随着信息化和数字化的快速发展，网络空间安全的重要性日益凸显，社会对网络安全人才的需求持续增长。网络空间安全专业注重多学科交叉，融合计算机科学、数学、通信工程、法律等学科知识，同时强调实践能力的培养，通过实验、实训、实习等方式提升学生的动手能力和解决实际问题的能力。学生将系统学习网络安全、系统安全、应用安全、信息内容安全等领域的知识，掌握密码学、网络攻防、安全协议、安全管理等核心技术，具备网络安全防护、漏洞分析、安全系统设计与开发、安全评估与管理的能力。本专业聚焦建设网络强国和保障网络安全急需，在夯实软件工程专业核心课程体系基础上，突出网络安全、密码学、网络攻击与防御等特色课程，着力培养兼具家国情怀、创新思维与实践能力的应用型高端人才。

二、培养目标（Program Objectives）

网络空间安全专业旨在响应建设网络强国和保障网络安全的迫切需求，秉承立德树人的教育理念，致力于培养德智体美劳全面发展，兼具深厚科学素养与人文素养的高素质人才。本专业的学生将具备扎实专业知识、坚实的数学与自然科学基础、出色工程实践能力、良好职业道德与团队协作能力，以及国际视野和终身学习能力。能够在政府机关、科研机构、企事业单位等部门成长为从事信息安全相关领域的科学研究、教学培养、安全设计、技术开发和安全管理等方面工作的应用型高端人才。

本专业毕业生毕业五年左右预期达成以下目标：

目标 1：具有健全人格、正确价值观和社会责任感，有工程报国、为民造福的意识，能够在工程实践中理解和践行工程伦理和职业规范。

目标 2：具有独立分析能力，在综合考虑健康、安全、环境、法律、经济和可持续发展等非技术因素影响下，能够运用跨学科知识和理论综合分析解决网络空间安全工程领域的复杂工程问题，能够参与或承担专业领域的研发项目，创新意识突出，并从健康、安全与环境、全生命周期成本与净零碳要求、法律与伦理、社会与文化等角度考虑可行性。

目标 3：具有良好的沟通技巧，能够快速融入团队；具有组织管理能力，能够成为工作团队中的骨干或领导者；具有国际视野和国际交流能力，理解、尊重语言和文化差异。

目标 4：具有继续学习能力和批判性思维，善于向实践学习，善于从实践中总结事物的规律性，不断更新调整自己的知识，能够理解广泛的技术变革对工程和社会的影响，适应新技术变革。

三、毕业要求（Graduation Requirements）

1. 工程知识：掌握扎实的数学、自然科学知识，以及密码学、网络安全、数据结构、数据库安全等核心专业课程知识，能够灵活运用这些知识解决网络安全领域的复杂工程问题。

2. 问题分析：能够运用数学、自然科学和工程科学的基本原理，识别、表述并分析网络安全领域的复杂问题。具备通过文献检索查询获取相关信息，分析并解决工程问题的能力。

3. 设计/开发解决方案：能够针对网络安全领域的复杂问题设计创新解决方案，根据特定需求进行网络安全软件模块或系统的设计与开发，并在设计过程中融入创新意识，综合考虑社会、健康、安全、法律、文化及环境等多重因素。

4. 研究：能够基于科学原理，采用科学方法，对网络安全领域的复杂问题进行研究，设计实验方案，收集、分析并解释数据，得出合理有效的结论。

5. 使用现代工具：能够针对网络安全问题，合理选择并熟练使用开发工具，运用软件资源进行预测与模拟，同时理解其局限性。

6. 工程与可持续发展：能够基于网络空间安全专业工程实践相关背景知识进行合理分析，评价专业工程实践和复杂工程问题解决方案对健康、安全、环境、法律以及经济和社会可持续发展的影响，并理解应承担的责任。

7. 工程伦理与职业规范：有工程报国、为民造福的意识，具有人文社会科学素养和社会责任感，能够理解和践行工程伦理，在工程实践中遵守工程职业道德、规范和相关法律，履行责任。

8. 个人和团队：能够在多样化、多学科背景下的团队中承担个体、团队成员以及负责人的角色。明确自己的责任，处理好成员间的竞争与合作关系，维护团队利益。

9. 沟通：具备出色的表达能力，能够就网络安全问题与同行及公众进行有效的书面和口头沟通。熟练掌握外语，具备国际视野，能在跨文化环境中交流。

10. 项目管理：掌握工程管理原理和经济决策方法，理解网络安全工程中的经济与管理因素，并能在多学科环境中应用。

11. 终身学习：具备自主学习和终身学习的意识，能够紧跟网络安全领域的发展动态，持续学习和适应行业变化。

四、培养目标与毕业要求关系矩阵（Relationship Matrix of Program Objectives and Graduation Requirements）

培养目标 毕业要求	培养目标1	培养目标2	培养目标3	培养目标4
毕业要求1	√	√		
毕业要求2	√	√		
毕业要求3	√	√	√	
毕业要求4	√	√	√	
毕业要求5	√	√		√

毕业要求 \ 培养目标	培养目标1	培养目标2	培养目标3	培养目标4
毕业要求6			√	√
毕业要求7		√	√	
毕业要求8				√
毕业要求9				√
毕业要求10	√	√		√
毕业要求11	√			√

五、主干学科（Main Disciplines）

网络空间安全

六、核心课程（Core Courses）

信息安全数学基础、Python 程序设计、网络安全法律法规、数据结构与算法、计算机网络、数据库原理及安全、网络安全、人工智能及安全、网络安全项目管理、网络攻击与防御、操作系统、密码学等。

七、主要集中性实践教学环节（Centralized Practice Teaching）

Python 程序设计课程设计、数据结构与算法课程设计、网络安全课程设计、人工智能及安全课程设计、网络攻击与防御课程设计、密码学课程设计、毕业实习、毕业设计（论文）等。

八、学制与学位授予类型（Duration & Degree Granted）

学制（Duration）： 四年（Four Years）

学位授予类型（Degree Granted）： 工学学士（Bachelor of Engineering）

九、学分学时结构

板块	类别		学时数（周数）	学分数	小计	
					学分数	比例（%）
理论教学板块	必修	公共课程	912	54	92	53.8
		专业课程	696	38		
	选修	公共课程（校本通识课）	160	10	26	15.2
		专业课程	256	16		

板块	类别		学时数（周数）	学分数	小计	
					学分数	比例（%）
实践教学板块	必修	公共课程	288+2 周	12	51	29.8
		专业实验	352	11		
		实习实践	38 周	27		
		创新实践与劳动技能	32	1		
	选修	专业实验	0	0	2	1.2
		创新实践与劳动技能	64	2		
合计			2760+40 周	171	171	100

十、毕业要求实现矩阵（Relationship Matrix of Curriculum and Graduation Requirements）

毕业要求	指标点	支撑课程	支撑强度
毕业要求 1—工程知识：掌握扎实的数学、自然科学知识，以及密码学、网络安全、数据结构、数据库安全等核心专业课程知识，能够灵活运用这些知识解决网络安全领域的复杂工程问题。	1.1：掌握数学、自然科学的知识，能将其应用于网络空间安全领域。	高等数学	H
		大学物理	M
		线性代数	M
		概率论与数理统计	M
		信息安全数学基础	M
	1.2：掌握密码学、数据结构、数据库安全等核心专业课程知识。	密码学	H
		数据结构与算法	H
		计算机网络	H
		数据库原理及安全	H
		操作系统	M
	1.3：掌握网络空间安全及相关工程领域的专业知识，能够将其应用于解决网络空间安全领域中的复杂问题。	人工智能及安全	H
		物联网安全	H
		数据安全与隐私保护	H
		云计算及安全	H
		工业互联网安全	H
		机器学习	M
毕业要求 2—问题分析：能够运用数学、自然科学和工程科学的基本原理，识别、表述并分析网络安全领域的复杂问题。具备通过文献检索查询获取相关信息，分析并解决工程问题的能力。	2.1：能够运用数学、自然科学和网络空间安全知识的基本原理，对网络空间安全中的相关领域及具体对象或环节进行识别。	高等数学	H
		网络空间安全导论	H
		计算机网络	H
		网络安全	H
		信息安全数学基础	H
	2.2：能够基于科学原理和数学模型方法对网络空间安全专业的复杂工程问题进行分析。	人工智能及安全	H
		物联网安全	H
		无线网络安全	H
		数据安全与隐私保护	M
		网络攻击与防御	M
		机器学习	M

毕业要求	指标点	支撑课程	支撑强度
	2.3：能够综合运用网络空间安全工程专业知识，借助文献研究获取相关信息，分析复杂工程问题的影响因素，寻求解决问题的多种途径，并能够获得有效结论。	毕业设计（论文）	H
		机器学习	M
		大数据技术	M
		区块链技术	M
		毕业实习	M
毕业要求3—设计/开发解决方案：能够针对网络安全领域的复杂问题设计创新解决方案，根据特定需求进行网络安全软件模块或系统的设计与开发，并在设计过程中融入创新意识，综合考虑社会、健康、安全、法律、文化及环境等多重因素。	3.1：能够针对网络空间安全领域的复杂问题提出并设计解决方案。	网络空间安全导论	H
		高等数学	H
		网络安全	H
		信息安全数学基础	H
		区块链技术	M
		大数据技术	M
	3.2：根据网络空间安全中的特定需求进行网络安全软件模块或系统的设计与开发，并综合考虑社会、健康、安全、法律、文化及环境等多重因素。	Python 程序设计	H
		毕业设计（论文）	H
		毕业实习	H
		网络空间安全综合实训	H
		数据结构与算法	M
		网络安全法律法规	M
	3.3：能够对网络空间安全软件模块或系统的设计与开发的过程中融入创新意识。	毕业设计（论文）	H
		毕业实习	H
		网络空间安全综合实训	H
		专业创造性劳动（大学生创新创业训练、学科竞赛、专利发明、软件著作权、学术论文）	M
毕业要求4—研究：能够基于科学原理，采用科学方法，对网络安全领域的复杂问题进行研究，设计实验方案，收集、分析并解释数据，得出合理有效的结论。	4.1：能够基于科学原理，通过采用科学方法，对网络安全领域的复杂问题进行研究。	人工智能及安全	H
		物联网安全	H
		无线网络安全	M
		数据安全与隐私保护	M
		图像处理与信息隐藏	M
		网络攻击与防御	M

毕业要求	指标点	支撑课程	支撑强度
	4.2：能够基于科学原理，通过采用科学方法，对网络安全领域的复杂问题设计实验方案，通过收集、分析并解释实验数据，得出合理有效的结论。	数据结构与算法课程设计	H
		网络安全课程设计	H
		人工智能及安全课程设计	H
		网络攻击与防御课程设计	H
		密码学课程设计	H
		Python 程序设计实验、数据结构与算法实验、计算机网络实验、数据库原理及安全实验、网络安全实验、人工智能及安全实验、网络攻击与防御实验、操作系统实验、密码学实验	M
毕业要求 5—使用现代工具：能够针对网络安全问题，合理选择并熟练使用开发工具，运用软件资源进行预测与模拟，同时理解其局限性。	5.1：针对不同的网络安全问题，能够使用现代工具进行网络安全分析。	网络安全	H
		网络安全课程设计	M
		人工智能及安全课程设计	M
		网络攻击与防御课程设计	M
		机器学习	L
	5.2：针对网络安全问题，能够合理选择并熟练使用开发工具。	网络安全	H
		网络安全课程设计	H
		Python 程序设计课程设计	M
	5.3：能够使用开发工具进行预测与模拟，能够评估工具的使用效果，理解其局限性。	毕业设计（论文）	H
		网络空间安全综合实训	H
		网络安全课程设计	M
		人工智能及安全课程设计	M
		网络攻击与防御课程设计	M
		计算机网络实验	M
毕业要求 6—工程与可持续发展：能够基于网络空间安全专业工程实践相关背景知识进行合理分析，评估专业工程实践和复杂工程问题解决方案对健康、安全、	6.1：基于网络空间安全及相关领域的技术标准体系、知识产权、产业政策和法律法规，能够评估网络安全解决方案对社会的影响。	思想道德与法治	H
		网络安全法律法规	H
		兴趣技能性劳动	M
		社会公益性劳动	M
	6.2：能够对网络空间安全专业工程实践相关背景知识进行合理分析，评估网络空间安全解	毕业实习	H
		思想道德与法治	H

毕业要求	指标点	支撑课程	支撑强度
环境、法律以及经济和社会可持续发展的影响，并理解应承担的责任。	决方案对健康、安全、环境和社会可持续发展的影响，并理解应承担的责任。	网络安全法律法规	H
		网络空间安全导论	M
		心理健康与安全教育	M
毕业要求7—工程伦理与职业规范：有工程报国、为民造福的意识，具有人文社会科学素养和社会责任感，能够理解和践行工程伦理，在工程实践中遵守工程职业道德、规范和相关法律，履行责任。	7.1：具备良好的人文社会科学素养，具有正确的世界观、人生观和价值观，具有健康的体质和良好的心理素质。	思想道德与法治	H
		中国近现代史纲要	H
		新生研讨课	M
		体育	M
		心理健康与安全教育	M
		国家安全教育	M
		实验室安全	M
		大学生职业生涯规划	M
	7.2：理解社会主义核心价值观，了解国情，具有建设祖国与服务社会的强烈责任感；在工程实践中能自觉遵守职业道德和规范，履行责任。	马克思主义基本原理	H
		毛泽东思想和中国特色社会主义理论体系概论	H
		习近平新时代中国特色社会主义思想概论	H
		毕业实习	M
		中国近现代史纲要	M
		形势与政策	L
毕业要求8—个人和团队：能够在多样化、多学科背景下的团队中承担个体、团队成员以及负责人的角色。明确自己的责任，处理好成员间的竞争与合作关系，维护团队利益。	8.1：能够正确认识团队力量和智慧，理解和处理多样化、多学科背景下个人和团队的关系。	专业创造性劳动（大学生创新创业训练、学科竞赛、专利发明、软件著作权、学术论文）	H
		网络安全项目管理	H
		大学生创新创业与就业指导	H
		体育	M
		劳动教育	M
		军事理论	L
	8.2：在多学科背景下，能够与团队成员进行有效的沟通与交流，胜任团队成员或团队负责人的角色并承担相应责任。	毕业设计（论文）	H
		网络安全项目管理	H
		大学生创新创业与就业指导	M
		毕业实习	M
		军事训练	L

毕业要求	指标点	支撑课程	支撑强度
毕业要求9—沟通：具备出色的表达能力，能够就网络安全问题与同行及公众进行有效的书面和口头沟通。熟练掌握外语，具备国际视野，能在跨文化环境中交流。	9.1：具有总结、归纳、整理并阐述网络空间安全专业复杂工程问题的能力，以口头、文稿、图表等方式与业界同行及社会公众进行有效沟通和交流。	毕业设计（论文）	H
		网络安全项目管理	H
		大学英语	M
		社会公益性劳动	M
	9.2：具备一定的外语口头和书面表达能力，能够阅读和理解本专业的外文文献，了解网络空间安全领域国际发展趋势和研究热点，具有一定的国际视野，能够在跨文化背景下进行沟通和交流，理解、尊重语言和文化差异。	大学英语	H
		毕业设计（论文）	H
		新生研讨课	M
毕业要求10—项目管理：掌握工程管理原理和经济决策方法，理解网络安全工程中的经济与管理因素，并能在多学科环境中应用。	10.1：了解工程及产品全周期、全流程的基本原理，掌握工程项目中涉及的管理原理与经济决策方法。	网络安全项目管理	H
		毕业实习	M
		毕业设计（论文）	M
	10.2：在多学科环境下，能够将工程管理和经济决策知识应用到网络空间安全工程问题的规划、方案产品设计和工程实施中。	网络安全项目管理	H
		毕业设计（论文）	H
		毕业实习	M
		专业创造性劳动（大学生创新创业训练、学科竞赛、专利发明、软件著作权、学术论文）	M
毕业要求11—终身学习：具备自主学习和终身学习的意识，能够紧跟网络安全领域的发展动态，持续学习和适应行业变化。	11.1：理解技术发展和进步对于知识和能力的影响和要求，对于自主学习、终身学习和批判性思维的必要性有正确的认识。	大学生职业生涯规划	H
		新生研讨课	H
		毕业实习	M
		习近平新时代中国特色社会主义思想概论	M
	11.2：具有自主学习的能力，能针对社会、职业和个人发展的需求，通过不断学习，提高归纳、凝练问题的能力和技术理解力，能够理解广泛的技术变革对工程和社会的影响，适应新技术变革。	毕业设计（论文）	H
		专业创造性劳动（大学生创新创业训练、学科竞赛、专利发明、软件著作权、学术论文）	H
		大学英语	M
		大学生职业生涯规划	M

注：课程对毕业要求支撑强度分别用“H（高）、M（中）、L（弱）”表示。

十一、理论教学计划（Theoretical Teaching Plan）

课程类别		课程名称	学分数	学时数	学期	教学周数	学时分配				考核方式			备注
							讲授	实验	实践	习题	考查	开卷	闭卷	
公共课程	必修	思想道德与法治	3	48	1	15	30		18				√	
		中国近现代史纲要	3	48	2	16	32		16				√	
		马克思主义基本原理	3	48	3	16	32		16				√	
		毛泽东思想和中国特色社会主义理论体系概论	3	48	4	16	32		16				√	
		习近平新时代中国特色社会主义思想概论	3	48	5	16	32		16				√	
		形势与政策	2	32	1-8	16	32				√			
		军事理论	2	32	1	16	32					√		
		大学英语 A1	2.5	48	1	16	32	16					√	
		大学英语 A2	2.5	48	2	16	32	16					√	
		大学英语 A3	2	48	3	16	16	32					√	
		大学英语 A4	2	48	4	16	16	32					√	
		高等数学 A1	6	96	1	16	96						√	
		高等数学 A2	6	96	2	16	96						√	
		线性代数	3	48	3	16	48						√	
		概率论与数理统计	3	48	3	16	48						√	
		大学物理 B1	4	64	2	16	64						√	
		大学物理 B2	4	64	3	16	64						√	

公共课程		课程类别	通识选修所含课程	必须修读的模块	任选模块课程
	选修	通识选修课：选修总学分至少为 10 学分	1. 文史哲经典与文化传承 2. 社会发展与现代性认识 3. 科技进步与科学认识 4. 艺术创作与审美体验 5. “四史”教育 6. 体育俱乐部（阳光体育运动） 7. 创新创业教育	1. 艺术创作与审美体验 2. “四史”教育四选一：党史、新中国史、改革开放史、社会主义发展史 3. 文史哲经典与文化传承 4. 创新创业教育	社会发展与现代性认识、科技进步与科学认识、体育俱乐部（阳光体育运动）
	以上要求必修 54 学分，选修 10 学分，共计 64 学分。				

课程类别		课程名称	学分数	学时数	学期	教学周数	学时分配				考核方式			备注
							讲授	实验	实践	习题	考查	开卷	闭卷	
专业课程	必修	新生研讨课	1	16	1	8	16				√			
		网络空间安全导论	3	48	1	16	48						√	H
		Python 程序设计	3	48	2	16	48						√	
		计算机网络	3	48	3	16	48						√	H
		数据库原理及安全	3	48	4	16	48						√	H
		数据结构与算法	3	48	4	16	48						√	H
		密码学	3	48	4	16	48						√	H
		信息安全数学基础	3	48	4	16	48						√	H
		操作系统	3	48	5	16	48						√	
		网络安全	3	48	5	16	48						√	H
		网络攻击与防御	3	48	6	16	48						√	H
		人工智能及安全	3	48	6	16	48						√	H
		网络安全项目管理	2	32	7	8	32						√	H
		网络安全法律法规	2	32	7	8	32						√	
	选修	物联网安全	2	32	5	16	24	8			√			
		网络工程	2	32	5	16	24	8			√			进阶课程
		机器学习	2	32	5	16	24	8			√			
		云计算及安全	2	32	6	16	24	8			√			
		数据安全与隐私保护	2	32	6	16	24	8			√			前沿课程
		区块链技术	2	32	6	16	24	8			√			交叉课程
		无线网络安全	2	32	7	16	24	8			√			
		专业外语	2	32	7	16	32				√			
		图像处理与信息隐藏	2	32	7	16	24	8			√			交叉课程
		大数据技术	2	32	7	16	24	8			√			进阶课程
		工业互联网安全	2	32	7	16	24	8			√			前沿课程
	以上必修 38 学分，选修 16 学分，共计 54 学分。													

十二、实践教学计划（Practical Teaching Plan）

课程类别		课程(项目)名称	学分数	学时数	学期	教学周数	考核方式	备注
公共课程	必修	军事训练	1		1	2	考查	
公共课程	必修	心理健康与安全教育	2		1-8		考查	
公共课程	必修	劳动教育	1	32	2	16	考查	
公共课程	必修	实验室安全	1	32	4	16	考查	
公共课程	必修	国家安全教育	1	32	1	16	考查	
公共课程	必修	体育 1	1	32	1	16	考查	
公共课程	必修	体育 2	1	32	2	16	考查	
公共课程	必修	体育 3	1	32	3	16	考查	
公共课程	必修	体育 4	1	32	4	16	考查	
公共课程	必修	体育 5	0.5	16	6	8	考查	
公共课程	必修	大学物理 B 实验	1.5	48	2/3	16	理论+操作	
公共课程	以上要求必修 10 学分，共计 10 学分。							
专业实验	必修	Python 程序设计实验	1	32	2	16	操作	
专业实验	必修	计算机网络实验	1	32	3	16	操作	
专业实验	必修	数据库原理及安全实验	1	32	4	16	操作	
专业实验	必修	数据结构与算法实验	1	32	4	16	操作	
专业实验	必修	密码学实验	1	32	4	16	操作	
专业实验	必修	操作系统实验	1	32	5	16	操作	
专业实验	必修	网络安全实验	1	32	5	16	操作	
专业实验	必修	网络攻击与防御实验	1	32	6	16	操作	
专业实验	必修	人工智能及安全实验	1	32	6	16	操作	
专业实验	以上要求必修 11 学分，选修 0 学分，共计 11 学分。							

<table>
<tr><th colspan="3">课程类别</th><th>课程(项目)名称</th><th>学分数</th><th>学时数</th><th>学期</th><th>教学周数</th><th>考核方式</th><th>备注</th></tr>
<tr><td rowspan="13">实习实践</td><td rowspan="12" colspan="2">必修</td><td>Python 程序设计课程设计</td><td>1</td><td></td><td>2</td><td>1</td><td>设计报告</td><td></td></tr>
<tr><td>计算机网络课程设计</td><td>1</td><td></td><td>3</td><td>1</td><td>设计报告</td><td></td></tr>
<tr><td>数据结构与算法课程设计</td><td>1</td><td></td><td>4</td><td>1</td><td>设计报告</td><td></td></tr>
<tr><td>密码学课程设计</td><td>1</td><td></td><td>4</td><td>1</td><td>设计报告</td><td></td></tr>
<tr><td>操作系统课程设计</td><td>1</td><td></td><td>5</td><td>1</td><td>设计报告</td><td></td></tr>
<tr><td>网络安全课程设计</td><td>1</td><td></td><td>5</td><td>1</td><td>设计报告</td><td></td></tr>
<tr><td>网络攻击与防御课程设计</td><td>1</td><td></td><td>6</td><td>1</td><td>设计报告</td><td></td></tr>
<tr><td>人工智能及安全课程设计</td><td>1</td><td></td><td>6</td><td>1</td><td>设计报告</td><td></td></tr>
<tr><td>网络空间安全综合实训</td><td>4</td><td></td><td>7</td><td>4</td><td>实训报告</td><td></td></tr>
<tr><td>网络空间安全专业生产实习</td><td>3</td><td></td><td>7</td><td>3</td><td>实习报告</td><td></td></tr>
<tr><td>毕业实习</td><td>4</td><td></td><td>8</td><td>4</td><td>实习报告</td><td></td></tr>
<tr><td>毕业设计（论文）</td><td>10</td><td></td><td>7-8</td><td>24</td><td>论文与答辩</td><td></td></tr>
<tr><td colspan="9">以上要求必修 27 学分，共计 27 学分。</td></tr>
<tr><td rowspan="13">创新实践与劳动技能</td><td rowspan="2" colspan="2">必修</td><td>大学生职业生涯规划</td><td>0.5</td><td>16</td><td>2</td><td></td><td>考查</td><td></td></tr>
<tr><td>大学生创新创业与就业指导</td><td>0.5</td><td>16</td><td>5</td><td></td><td>考查</td><td></td></tr>
<tr><td rowspan="9">选修</td><td rowspan="5">专业创造性劳动</td><td>大学生创新创业训练</td><td>2</td><td></td><td></td><td></td><td>项目参与证明或结项通知</td><td></td></tr>
<tr><td>学科竞赛</td><td>2</td><td></td><td>1-8</td><td></td><td>获奖证书</td><td></td></tr>
<tr><td>专利发明</td><td>2</td><td></td><td>1-8</td><td></td><td>专利证书</td><td></td></tr>
<tr><td>软件著作权</td><td>2</td><td></td><td>1-8</td><td></td><td>软著证书</td><td></td></tr>
<tr><td>学术论文</td><td>2</td><td></td><td>1-8</td><td></td><td>录用通知或 DOI 号</td><td></td></tr>
<tr><td>兴趣技能性劳动</td><td>技能培训</td><td>2</td><td></td><td>1-8</td><td></td><td>技能证书</td><td></td></tr>
<tr><td rowspan="2">社会公益性劳动</td><td>志愿者服务</td><td>1</td><td></td><td>1-8</td><td></td><td>志愿服务组织认定，时长不少于 32 小时</td><td></td></tr>
<tr><td>社会实践</td><td>1</td><td></td><td>1-8</td><td></td><td>学院或相关职能部门认定，时长不少于 32 小时</td><td></td></tr>
<tr><td colspan="8">以上要求必修 1 学分，选修 2 学分，共计 3 学分。</td></tr>
</table>

十三、教学进度表（Teaching Process Table）

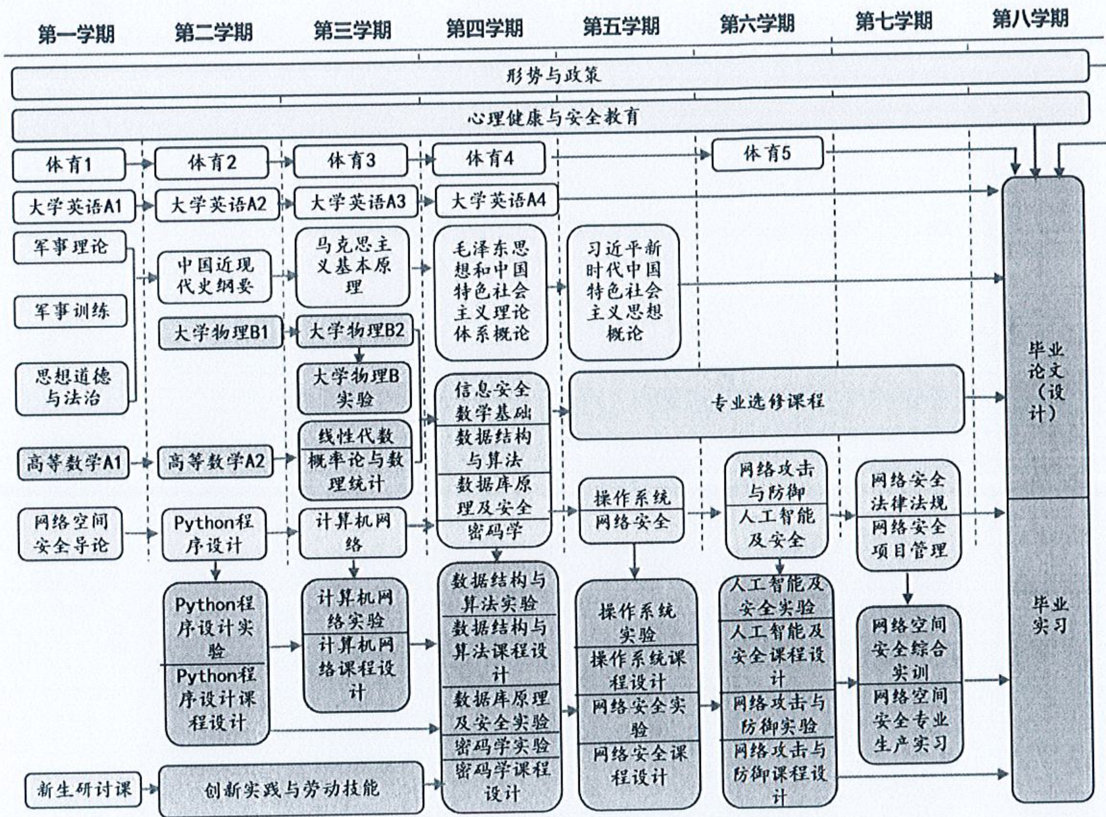
学期	类　别	课程（项目）名称	必修/选修	学分数	备注
1	理论教学	军事理论	必修	2	
		思想道德与法治	必修	3	
		大学英语 A1	必修	2.5	
		高等数学 A1	必修	6	
		网络空间安全导论	必修	3	
		新生研讨课	必修	1	
		形势与政策	必修	0.25	
	实践教学	军事训练	必修	1	
		国家安全教育	必修	1	
		心理健康与安全教育	必修	0.25	
		体育 1	必修	1	
	以上必修 20 学分，共计 20 学分。				
2	理论教学	中国近现代史纲要	必修	3	
		大学英语 A2	必修	2.5	
		高等数学 A2	必修	6	
		大学物理 B1	必修	4	
		Python 程序设计	必修	3	
		形势与政策	必修	0.25	
	实践教学	心理健康与安全教育	必修	0.25	
		劳动教育	必修	1	
		大学生职业生涯规划	必修	0.5	
		Python 程序设计课程设计	必修	1	
		Python 程序设计实验	必修	1	
		体育 2	必修	1	
	以上必修 23.5 学分，共计 23.5 学分。				

学期	类　别	课程（项目）名称	必修/选修	学分数	备注
3	理论教学	马克思主义基本原理	必修	3	
		大学英语 A3	必修	2	
		线性代数	必修	3	
		大学物理 B2	必修	4	
		概率论与数理统计	必修	3	
		计算机网络	必修	3	
		形势与政策	必修	0.25	
	实践教学	心理健康与安全教育	必修	0.25	
		体育 3	必修	1	
		大学物理 B 实验	必修	1.5	
		计算机网络课程设计	必修	1	
		计算机网络实验	必修	1	
	以上必修 23 学分，共计 23 学分。				
4	理论教学	毛泽东思想和中国特色社会主义理论体系概论	必修	3	
		大学英语 A4	必修	2	
		信息安全数学基础	必修	3	
		数据库原理及安全	必修	3	
		密码学	必修	3	
		数据结构与算法	必修	3	
		形势与政策	必修	0.25	
	实践教学	心理健康与安全教育	必修	0.25	
		体育 4	必修	1	
		实验室安全	必修	1	
		数据库原理及安全实验	必修	1	
		数据结构与算法实验	必修	1	
		数据结构与算法课程设计	必修	1	
		密码学实验	必修	1	
		密码学课程设计	必修	1	
	以上必修 23.5 学分，共计 23.5 学分。				

学期	类　别	课程（项目）名称	必修/选修	学分数	备注
5	理论教学	习近平新时代中国特色社会主义思想概论	必修	3	
		操作系统	必修	3	
		网络安全	必修	3	
		物联网安全	选修	2	
		网络工程	选修	2	
		机器学习	选修	2	
		形势与政策	必修	0.25	
	实践教学	大学生创新创业与就业指导	必修	0.5	
		心理健康与安全教育	必修	0.25	
		网络安全实验	必修	1	
		网络安全课程设计	必修	1	
		操作系统课程设计	必修	1	
		操作系统实验	必修	1	
	以上必修 14 学分，选修 4 学分，共计 18 学分。				
6	理论教学必修	网络攻击与防御	必修	3	
		人工智能及安全	必修	3	
		云计算及安全	选修	2	
		数据安全与隐私保护	选修	2	
		区块链技术	选修	2	
		形势与政策	必修	0.25	
	实践教学	心理健康与安全教育	必修	0.25	
		体育 5	必修	0.5	
		网络攻击与防御实验	必修	1	
		网络攻击与防御课程设计	必修	1	
		人工智能及安全实验	必修	1	
		人工智能及安全课程设计	必修	1	
	以上必修 11 学分，选修 4 学分，共计 15 学分。				

学期	类　别	课程（项目）名称	必修/选修	学分数	备注
7		网络安全项目管理	必修	2	
		网络安全法律法规	必修	2	
		无线网络安全	选修	2	
		专业外语	选修	2	
		图像处理与信息隐藏	选修	2	
		大数据技术	选修	2	
		工业互联网安全	选修	2	
		形势与政策	必修	0.25	
	实践教学	心理健康与安全教育	必修	0.25	
		网络空间安全专业生产实习	必修	3	
		网络空间安全综合实训	必修	4	
	以上必修 11.5 学分，选修 8 学分，共计 19.5 学分。				
8	理论教学	形势与政策	必修	0.25	
	实践教学	心理健康与安全教育	必修	0.25	
		毕业实习	必修	4	
		毕业设计（论文）	必修	10	
	以上必修 14.5 学分，共计 14.5 学分。				

十四、课程修读导图（Course Flow Chart）



6. 教师及课程基本情况表

6.1专业核心课程情况表

课程名称	课程总学时	课程周学时	拟授课教师	授课学期
新生研讨课	16	2	武俊生	1
网络空间安全导论	48	3	任焕荣	1
Python程序设计	48	3	白茹意	2
计算机网络	48	3	张举	3
数据库原理及安全	48	3	刘静	4
数据结构与算法	48	3	米晓萍	4
密码学	48	3	张润发	4
信息安全数学基础	48	3	池浩田	4
操作系统	48	3	王香云	5
网络安全	48	3	耿海军	5
网络攻击与防御	48	3	吴勇	6
人工智能及安全	48	3	杨静，郭雪	6
网络安全项目管理	32	2	杨亚芳	7
网络安全法律法规	32	2	刘三亚	7
物联网安全	32	2	朱云雷	5
网络工程	32	2	尹少平	5
机器学习	32	2	曹学飞	5
云计算及安全	32	2	王建荣	6
数据安全与隐私保护	32	2	孙美婷	6
区块链技术	32	2	霍金鉴	6
无线网络安全	32	2	王宇纬，张荣	7
专业外语	32	2	王玲	7
图像处理与信息隐藏	32	2	安凤平，郭小英	7
大数据技术及安全	32	2	杨建英	7
工业互联网安全	32	2	王金勇	7

6.2本专业授课教师基本情况表

姓名	性别	出生年月	拟授课程	专业技术职务	学历	最后学历毕业学校	最后学历毕业专业	最后学历毕业学位	研究领域	专职/兼

										职
耿海军	男	1983-08	网络安全	教授	研究生	清华大学	计算机科学与技术	博士	网络安全	专职
武俊生	男	1965-03	新生研讨课	教授	研究生	北京理工大学	火箭发动机	硕士	软件开发	专职
安凤平	男	1985-10	图像处理与信息隐藏	教授	研究生	北京科技大学	通信与信息系统	博士	深度学习	专职
曹学飞	男	1981-11	机器学习	副教授	研究生	山西大学	计算机科学与技术	博士	网络安全	专职
王宇纬	男	1994-06	无线网络安全	副教授	研究生	西安电子科技大学	机械工程	博士	网络安全	专职
张润发	男	1992-06	密码学	副教授	研究生	大连理工大学	软件工程	博士	人工智能，安全	专职
霍金鉴	男	1993-05	区块链技术	副教授	研究生	中国民航大学	安全科学与工程	博士	网络安全	专职
任焕荣	男	1995-09	网络空间安全导论	副教授	研究生	西安交通大学	机械工程	博士	人工智能安全	专职
郭小英	女	1985-01	图像处理与信息隐藏	副教授	研究生	广岛大学（日本）	信息工程	博士	计算机视觉安全	专职
张荣	男	1994-05	无线网络安全	副教授	研究生	东华大学	机械工程	博士	工业网络安全	专职
王建荣	男	1986-07	云计算及安全	副教授	研究生	北京科技大学	通信与信息系统	博士	复杂系统建模与优化	专职
刘三亚	女	1988-09	无线网络安全	副教授	研究生	厦门大学	通信与信息系统	博士	通信安全	专职
池浩田	男	1990-11	信息安全数学基础	副教授	研究生	美国天普大学	计算机与信息科学	博士	信息安全	专职
杨静	女	1990-02	人工智能及安全	副教授	研究生	西北工业大学	计算机科学与技术	博士	图像安全	专职
尹少平	男	1965-07	网络工程	副教授	研究生	中国科学院声学研究所	声学	硕士	网络安全	专职
王香云	女	1979-09	操作系统	副教授	研究生	太原理工大学	控制理论与控制工	硕士	软件安全	专职

							程			
吴勇	男	1981-10	网络攻击与防御	讲师	研究生	贵州大学	计算机软件与李理论	硕士	网络安全	专职
杨建英	女	1976-06	大数据技术及安全	讲师	研究生	华南师范大学	人工智能与模糊识别	硕士	算法与密码学	专职
张举	男	1972-03	计算机网络	讲师	研究生	中北大学	计算机应用技术	硕士	网络安全	专职
白茹意	女	1987-12	Python程序设计	讲师	研究生	北京师范大学	计算机应用技术	硕士	智能图像安全	专职
王金勇	男	1974-08	工业互联网安全	副教授	研究生	哈尔滨工业大学	计算机系统结构	博士	软件安全	专职
孙美婷	女	1992-09	数据安全与隐私保护	副教授	研究生	北京工业大学	控制科学与工程	博士	数据质量治理	专职
刘静	女	1990-09	网络安全法律法规	副教授	研究生	山西大学	计算机科学与技术	博士	人工智能安全	专职
米晓萍	女	1976-01	数据结构与算法	副教授	研究生	武汉水利电力大学	计算机科学与技术	硕士	物联网安全	专职
杨亚芳	女	1986-10	网络安全项目管理	讲师	研究生	西北工业大学	计算机技术	硕士	移动设备安全	专职
王玲	女	1980-06	专业外语	讲师	研究生	太原理工大学	计算机应用技术	硕士	网络安全	专职
朱云雷	男	1985-08	物联网安全	讲师	研究生	计算机应用技术	计算机应用技术	硕士	软件安全	专职
郭雪	女	1987-02	人工智能及安全	讲师	研究生	北京理工大学	计算机技术	硕士	人工智能安全	专职

6.3教师及开课情况汇总表

专任教师总数	28		
具有教授（含其他正高级）职称教师数	3	比例	10.71%
具有副教授及以上（含其他副高级）职称教师数	20	比例	71.43%
具有硕士及以上学位教师数	28	比例	100.00%
具有博士学位教师数	16	比例	57.14%
35岁及以下青年教师数	9	比例	32.14%

36-55岁教师数	17	比例	60.71%
兼职/专职教师比例	0:28		
专业核心课程门数	25		
专业核心课程任课教师数	28		

7. 专业主要带头人简介

姓名	耿海军	性别	男	专业技术职务	教授	行政职务	系主任
拟承担课程	网络安全			现在所在单位	山西大学		
最后学历毕业时间、学校、专业	2015年毕业于清华大学计算机科学与技术系						
主要研究方向	网络安全						
从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）	2025年获山西省高校网络教育名师，2025年获批山西省研究生线下优质课程，2025年指导学生获批大学生创新训练计划项目国家级项目，2025年指导学生获得第十六届蓝桥杯全国软件和信息技术专业人才大赛全国总决赛二等奖，2025年指导学生获得全国高校商业精英挑战赛品牌策划竞赛全国总决赛二等奖，2024年获批中国高校产学研创新基金，2023年第十八届“挑战杯”全国大学生课外学术科技作品竞赛铜奖，2023年获批山西省高等学校本科教学改革创新项目，2022年获批教育部协同育人项目，2022年获批山西省研究生优秀教学案例库建设项目，发表教学改革论文4篇，出版教材4部，出版专著1部。						
从事科学研究及获奖情况	山西省“三晋英才”青年优秀人才，主持国家自然基金面上项目1项，青年基金项目1项，山西省高等学校科技创新项目1项，在TON、TPDS、INFOCOM、Neurocomputing、JNCA、Computer Networks、Tsinghua Science and Technology、软件学报和计算机研究与发展等国际国内重要学术刊物和会议上发表学术论文20余篇，授权中国发明专利20余项。						
近三年获得教学研究经费（万元）	16.0			近三年获得科学研究经费（万元）	200.0		
近三年给本科生授课课程及学时数	授课网络及其计算 学时48*3=144 授课程序设计基础 学时32*3=96			近三年指导本科毕业设计（人次）	76		

姓名	曹学飞	性别	女	专业技术职务	副教授	行政职务	副系主任
拟承担课程	网络安全			现在所在单位	山西大学		

最后学历毕业时间、学校、专业	2020年毕业于山西大学计算机科学与技术系		
主要研究方向	网络安全		
从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）	2025年指导学生获得第十六届蓝桥杯全国软件和信息技术专业人才大赛全国总决赛一等奖，2024年获批获批山西省线下一流课程，2024年指导学生获批大学生创新训练计划项目国家级项目，2024年获山西省高等学校本科教学改革创新项目，2023年指导学生获得华北五省(市、自治区)及港澳台大学生计算机应用大赛一等奖，2021年获批教育部协同育人项目，发表教学改革论文3篇，出版教材1部。		
从事科学研究及获奖情况	在Pattern Recognition Letters、应用概率统计等国际国内重要学术刊物和会议上发表学术论文10余篇，授权发明专利2项。		
近三年获得教学研究经费（万元）	15.0	近三年获得科学研究经费（万元）	95.0
近三年给本科生授课课程及学时数	授课计算机系统基础 学时48*3=144	近三年指导本科毕业设计（人次）	74

姓名	郭小英	性别	男	专业技术职务	副教授	行政职务	副系主任
拟承担课程	图像处理与信息隐藏			现在所在单位	山西大学		
最后学历毕业时间、学校、专业	2014年毕业于广岛大学（日本）信息工程系						
主要研究方向	计算机视觉安全						
从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）	2025年获山西省高等学校本科教学改革创新项目，2023年获批山西省线下一流课程，2023年获山西省高等学校本科教学改革创新项目，2023年获得省级第三届创新教学比赛三等奖，2021年获批山西省研究生优秀教学案例库建设项目，2021年获得山西省课程思政教学设计大赛三等奖，发表教学改革论文4篇，出版专著1部。						
从事科学研究及获奖情况	山西省“三晋英才”青年优秀人才，主持国家自然基金青年基金项目1项，山西省基础研究计划自然科学研究面上项目1项，山西省高等学校科技创新项目1项，山西省回国留学人员科研教研资助项目1项，在Knowledge-based System、OPTICAL REVIEW、电子学报、中国图象图象学报等国际国内重要学术刊物和会议上发表学术论文20余篇。						

近三年获得教学研究经费（万元）	13.0	近三年获得科学研究经费（万元）	70.0
近三年给本科生授课课程及学时数	授课数字图像处理技术 学时 32*3*3=288	近三年指导本科毕业设计（人次）	58

8. 教学条件情况表

可用于该专业的教学实验设备总价值（万元）	486.92	可用于该专业的教学实验设备数量（千元以上）	576（台/件）
开办经费及来源	60万/年，山西大学拨款。		
生均年教学日常运行支出（元）	4000.0		
实践教学基地（个）	5		
教学条件建设规划及保障措施	学校和学院教学设备完善，多媒体教室充足，设备现代化程度高，山西大学教务处对于“网络空间安全”新专业的开办进行资助，保障专业开办期间各项发展条件完备和充足。 学校图书馆是全国古籍重点保护单位，馆藏图书256.39万册，数字资源1547.95万册，数据库212个。 学院拥有完备的计算机专业实验中心及高效教学云平台，计算机专业试验室9个，建筑面积2250多平方米，服务器、台式机及各种计算机设备，可以有效支撑教学的开展。		

主要教学实验设备情况表

教学实验设备名称	型号规格	数量	购入时间	设备价值（千元）
教学资源管理服务器	PowerEdge R430	1	2017	39.0
网络信息安全实训室综合管理平台	V1.0	1	2017	34.0
网络信息安全教学资源统一标识	V1.0	1	2017	31.0
TCL智能会议平板	TCL LE65X10TC	1	2018	28.0
图型工作站	ThinkStation P720	1	2019	40.0
信息安全云实验系统	V2.0	1	2020	100.0
专用服务器	R620 G30	6	2021	152.0
云桌面计算节点	YS26	5	2021	375.0
计算机	启天M430-B678	375	2021	2220.0
计算机	YX4200F	150	2021	290.0
桌面虚拟化软件	OIP232-1170	1	2021	135.0
光电交换机	C1000-24T-4X-L	12	2021	88.0
光电交换机	S5130S-28P-EI-HI	5	2023	18.0

光电交换机	IS230-28TF-AC	4	2023	18.0
光电交换机	IS420-36GTXF-AC	1	2023	4.0
教育桌面云软件	OIP232-1170	1	2023	734.0
教学管理系统	噢易多媒体网络教室软件V9.0	1	2023	66.0
网络与信息安全管理员课程	V1.0	1	2023	57.0
网路与信息安全管理员题库	V1.0	1	2023	38.0
教学云平台	噢易V5.0	1	2023	96.0
专用服务器	2288HV5	1	2023	29.0
管理云支撑终端	OIP832-1170	3	2023	169.0
管理服务器	JY-GLFQ-01	1	2023	62.0
运维安全审计系统	GD-OSA-M1000	1	2024	48.0

9. 申请增设专业的理由和基础

申请增设专业的理由和基础

一、增设专业的必要性

网络空间已成为继陆、海、空、天之后的第五大主权领域空间，其安全问题直接关系到国家安全、社会稳定以及个人隐私保护等诸多重要方面。在当今数字化时代，网络攻击、数据泄露等安全事件频发且愈发严重，给国家、企业和个人带来了不可估量的损失。据国际信息系统安全认证联盟发布的《2023 年全球网络安全人才发展报告》显示，全球网络安全人才规模达到 550 万人，同比增长 8.7%，然而人才缺口却进一步扩大到 400 万人，平均增长 12.6%，特别是在亚太地区，网络安全人才短缺人数同比增长 23.4%。而我国网络安全人才供需失衡问题更为严峻，据教育部发布的《网络安全人才实战能力白皮书》指出，预计到 2027 年，我国网络安全人员缺口将达到 327 万，而高校每年的人才培养规模仅为 3 万。面对如此庞大的人才需求缺口，山西大学增设网络空间安全专业显得尤为必要。这不仅是对国家战略需求的积极响应，能够为国家培养出一批具备扎实理论基础、较强实践能力和创新精神的专业人才，服务于网络强国建设，保障国家网络安全和信息安全，同时也契合了行业发展趋势，为地方经济建设和行业发展输送急需的专业人才，推动区域经济的数字化转型和高质量发展。

山西大学增设网络空间安全专业的计划紧密契合国家战略需求、行业发展趋势以及学校自身的学科布局规划。从宏观层面来看，随着信息技术的飞速发展，网络空间安全已成为国家安全战略中的关键一环，国家对网络安全专业人才的需求迫在眉睫，山西大学增设该专业能够为国家培养出一批具备扎实理论基础、较强实践能力和创新精神的专业人才，为网络强国建设提供有力的人才支撑。从行业需求角度分析，当前全球数字经济蓬勃发展，各关键行业对网络空间安全的重视程度不断提高，对网络安全专业人才的需求呈现出爆发式增长，而高校现有的人才培养规模远远不能满足市场需求。山西大学增设网络空间安全专业，能够为地方经济建设和行业发展培养急需的专业人才，促进区域经济的数字化转型和高质量发展。从学校自身发展来看，山西大学作为一所学科门类齐全的综合性大学，在多个学科领域都具有较高的教学和科研水平。增设网络空间安全专业将进一步完善学校的信息学科布局，促进学科间的交叉融合与协同发展。网络空间安全专业与学校的计算机科学与技术和软件工程等相关学科紧密相连，相互支撑。通过整合优势资源，学校可以在网络空间安全领域形成从本科到硕士、博士的完整人才培养体系，提升学校在网络空间安全领域的学科影响力和综合实力。

二、山西大学的建设基础

（一）学科平台优势

山西大学于 2019 年获批网络空间安全一级学科硕士学位授权点，成为山西

省首批拥有该授权点的高校之一。学校在网络空间安全领域已构建起较为完善的学科平台体系，包括 2 个省级工程技术研究中心、2 个省级研究生教育创新中心、1 个省级创新团队以及 2 个山西省国际合作基地与平台项目。这些优质平台为师生提供了广阔的科研空间和丰富的实践机会，极大地推动了网络空间安全学科的建设和发展。山西大学的计算智能与中文信息处理教育部重点实验室、复杂系统与数据科学教育部重点实验室等，为开展前沿性的网络空间安全研究提供了坚实的基础和良好的科研条件。

（二）师资队伍实力

学校在网络空间安全学位点领域汇聚了一支高水平师资队伍，现有专任教师 21 名，其中教授 5 名，博导 3 名，硕导 18 名，具有博士学位的教师 18 名，获外单位硕士及以上学位的比例为 85.71%，35 岁及以下有 6 人，比例为 28.57%。教师们在网络安全领域具有深厚的学术造诣，已在国内外学术期刊和会议上发表了多篇高质量的学术论文，并主持了多项国家级和省级科研项目，为网络空间安全专业的教学和科研提供了有力保障。

（三）教学资源与实践条件

学校高度重视网络空间安全专业的教学资源建设，配备了先进的实验教学设备和专业软件，建设了包括集群 NAS 存储系统、数据中心平台、高性能计算平台、网络攻防演练平台、软件定义网络平台等在内的多个高水平实验室。这些实验室为学生提供了理论与实践相结合的学习环境，使学生能够在实际操作中掌握网络空间安全的核心技术和技能。此外，学校与北京天融信教育科技有限公司等一流网络安全企业建立了长期稳定的合作关系，为学生提供了丰富的实践教学基地和就业机会。学校与企业共建的校外实践基地，为学生提供了参与实际网络安全项目的实践机会，有效提升了学生的实践能力和解决实际问题的能力。

（四）人才培养成果

网络空间安全学位点致力于培养 “高层次应用型创新人才”，重视学生创新意识与实践能力培养。首届硕士研究生学位论文盲审合格率 100%，顺利毕业且 100% 就业，就业领域广泛，体现学科培养的普适性与实用性，且学科积极支持研究生到国外高水平大学联合培养，2024 年 10 月已经选派 3 名研究生前往奥克兰大学进行联合培养。

为激发研究生学术兴趣等，学位点在多层面建立规定要求及激励机制，提供良好条件，如组织参加学科竞赛、选拔参加联合培养、鼓励参与科研项目等。近三年，研究生发表 SCI/EI、中文核心等学术论文 30 余篇，申请专利 20 余项，获各类学科竞赛奖 10 余项，综合素质显著提升，学位点的持续创新力和竞争力也得到增强。

（五）学科方向与发展

山西大学网络空间安全学科已形成网络与系统安全、应用与数据安全及新型信息技术安全两大研究方向。在网络与系统安全方面，主要研究工业控制系统的网络安全态势感知与防御、工业控制系统软件安全等，针对工业控制系统网络安全系统存在的漏洞难发现、攻击难溯源、防护易突破等挑战，研发工业控制系统网络攻击的防护技术，搭建相应的网络安全态势感知与防护平台。在应用与数据安全及新型信息技术安全方面，主要研究物联网和智能设备在信息物理系统中的安全与隐私保护，针对山西省智能制造、智慧城市、智能家居和无人系统等技术领域，解决复杂系统中的设备交互逻辑复杂性、安全脆弱性累积风险和设备管理策略的冲突问题，研发集成监控和干预的综合平台，提升数据安全性。学科还保持与国内外顶尖学者在新型电力系统、物联网和智能设备等关键领域的合作与交流，确保在网络空间安全研究领域的前瞻性和技术开发的实力性，培养的人才能够满足市场需求。

三、增设专业的意义和前景

（一）对人才培养的意义

增设网络空间安全专业将为学生提供一个系统学习网络空间安全知识和技能的平台，使学生能够深入掌握网络空间安全领域的基本理论和方法，具备扎实的专业知识和技能。通过专业学习，学生将具备较强的网络攻防实战能力、安全系统设计与开发能力以及安全策略制定与实施能力，能够适应网络空间安全领域的科研机构、高校、企业、政府机关等单位的工作需求。同时，学校注重培养学生的科学素养和创新意识，使学生能够跟踪网络空间安全领域的前沿技术和发展动态，开展前沿性的科研工作。此外，学校还注重培养学生的团队协作精神和沟通能力，使学生能够在跨学科、跨领域的团队中发挥作用，共同解决复杂的网络空间安全问题。

（二）对学生就业的意义

随着网络空间安全行业的发展，对专业人才的需求不断增长，为学生提供了广阔的就业空间和发展机会。山西大学网络空间安全专业的学生在毕业后，凭借在学校所学的专业知识和技能，将能够在各大企事业单位、政府部门从事网络安全相关工作，如网络安全工程师、渗透测试工程师、安全咨询顾问等职位。学校与多家知名企业的合作关系也将为学生提供更多的就业机会和职业发展空间，提高学生的就业竞争力。

（三）对学校和社会的意义

增设网络空间安全专业将进一步提升山西大学在网络空间安全领域的学科影响力和综合实力，为学校的发展注入新的活力。同时，该专业的建设也将为社

会培养出更多优秀的网络空间安全专业人才，满足国家对网络安全人才的迫切需求，为维护国家网络安全和社会稳定做出积极贡献。此外，学校通过开展网络空间安全教育和科研，将推动网络空间安全技术的发展和创新，为网络空间安全产业的发展提供技术支持和智力保障。

综上所述，山西大学增设网络空间安全专业具有充分的理由和扎实的基础，学校将充分发挥自身的综合优势，加大对网络空间安全专业的建设投入，努力将该专业打造成国内一流、具有一定国际影响力的专业，为国家和社会培养更多优秀的网络空间安全专业人才，为推进网络强国建设和数字经济发展贡献山西大学的力量。

10. 校内专业设置评议专家组意见表



校内专业设置评议专家组意见表

总体判断拟开设专业是否可行	☑是　□否

理由：

2025年5月16日，山西大学自动化与软件学院组织相关专家召开了“网络空间安全”本科专业申报论证会。评审组由来自清华大学、中国电子科技集团公司第三十三研究所、太原理工大学、太原科技大学、山西师范大学、山西财经大学和山西大学等单位的 7 名专家组成。与会专家听取了山西大学“网络空间安全”专业申报小组的汇报，审阅了相关申报材料，经过充分的交流和严谨的论证，形成评议意见如下：

1、山西大学开设“网络空间安全”专业契合国家战略安全需求及山西省数字经济发展趋势。

2、开设“网络空间安全”专业的基本条件满足本科专业类教学质量国家标准。

3、该专业教师团队在网络安全领域取得了较好的研究成果，具备丰富的教学与科研经验，能够为专业开设与发展提供有力保障。

4、拟招生人数 70 名，与该专业人才市场需求及学校教学资源承载能力相匹配，符合人才需求预测水平。

5、实践教学条件达到开设该专业的要求，专业建设经费较为充足。

6、山西大学计算机科学与技术和软件工程都是国家级一流本科专业，与网络空间安全专业紧密相连、相互支撑，可为“网络空间安全”专业的开设提供坚实的基础。

专家组一致同意山西大学申报“网络空间安全”本科专业。

拟招生人数与人才需求预测是否匹配		☑是　□否
本专业开设的基本条件是否符合教学质量国家标准	教师队伍	☑是　□否
	实践条件	☑是　□否
	经费保障	☑是　□否

专家签字：杨永海　马俊明　陈永乐　崔志华　王清　常利伟　郭丽峰